大数据的安全理解及应对策略研究

胡　坤[1],刘　镝[2],刘明辉[2]

(1.中国联合网络通信集团有限公司博士后科研工作站　北京 100033;
2.中国联通研究院平台与云计算研究中心　北京 100032)

摘　要:大数据以浅显易懂的概念、广泛潜在的应用需求和可展望的巨大经济效益,成为继移动互联网、云计算、物联网之后信息技术领域的又一热点。但是,随之而来的数据安全和隐私保护问题给大数据发展带来相应的挑战。梳理了各领域的大数据安全需求,分析了大数据环境下的安全特征与问题,提炼出大数据的安全内涵,最后给出了相应的发展策略。

关键词: 大数据安全;安全内涵;应对策略

doi: 10.3969/j.issn.1000-0801.2014.02.015

Research on Security Connotation and Response Strategies for Big Data

Hu Kun[1], Liu Di[2], Liu Minghui[2]

(1. Postdoctoral Workstation, China United Network Communications Corporation Limited, Beijing 100033, China;
2. Platform and Cloud Computing Research Center, China Unicom Labs, Beijing 100032, China)

Abstract: Big data is easy to understand which has many potential application requirements and foreseeable enormous economic benefits. With the development of mobile internet, cloud computing and M2M, big data become a new focus in the information technology field. But, it brings some challenges and problems, such as data security and privacy protection. The security requirements of big data in various fields were reviewed, and the security features and problems in big data environment were analyzed. Then the security connotation of big data was summarized and some response strategies were proposed.

Key words: big data security, security connotation, response strategy

1　引言

大数据的产生使数据分析与应用更加复杂，难以管理。据统计,过去 3 年里全球产生的数据量比以往 400 年的数据加起来还多,这些数据包括文档、图片、视频、Web 页面、电子邮件、微博等不同类型,其中,只有 20%是结构化数据,80%则是非结构化数据[1]。数据的增多使数据安全和隐私保护问题日渐突出,各类安全事件给企业和用户敲醒了警钟。在整个数据生命周期里,企业需要遵守更严格的安全标准和保密规定,对数据存储与使用的安全性和隐私性要求越来越高,传统数据保护方法常常无法满足新变化。网络和数字化生活也使黑客更容易获得他人信息,有了更多不易被追踪和防范的犯罪手段,而现有的法律法规和技术手段却难于解决此类问题。因此,在大数据环境下数据安全和隐私保护是一个重大挑战。

但是也应该看到,在大数据时代,业务数据和安全需求相结合能够有效提高企业的安全防护水平。通过对业务数据的大量搜集、过滤与整合,经过细致的业务分析和关

联规则挖掘，企业能够感知自身的网络安全态势，预测业务数据走向，了解业务运营安全情况，这对企业来说具有革命性的意义。目前，在一些运营商的业务部门已经开始使用安全基线和大数据分析技术，及时检测与发现网络中的各种异常行为和安全威胁，从而采取相应的安全措施。据 Gartner 公司预测，2016 年 40%的企业（以银行、保险、医药、电信、金融和国防等行业为主）将积极地对至少 10 TB 数据进行分析，以找出潜在的安全危险[2]。

随着对大数据的广泛关注，有关大数据安全的研究和实践也已逐步展开，包括科研机构、政府组织、企事业单位、安全厂商等在内的各方力量，正在积极推动与大数据安全相关的标准制定和产品研发，为大数据的大规模应用奠定更加安全和坚实的基础。

2 不同领域的大数据安全需求

在理解大数据安全内涵、制定相应策略之前，有必要对各领域大数据的安全需求进行全面了解和掌握，以分析大数据环境下的安全特征与问题。

（1）互联网行业

互联网企业在应用大数据时，常会涉及数据安全和用户隐私问题。随着电子商务、手机上网行为的发展，互联网企业受到攻击的情况比以前更为隐蔽，攻击的目的并不仅是让服务器宕机，更多是以渗透 APT 的攻击方式进行。因此，防止数据被损坏、篡改、泄露或窃取的任务十分艰巨。同时，由于用户隐私和商业机密涉及的技术领域繁多、机理复杂，很难有专家可以贯通法理与专业技术，界定出由于个人隐私和商业机密的传播而产生的损失，也很难界定侵权主体是出于个人目的还是企业行为。因此，互联网企业的大数据安全需求是：可靠的数据存储，安全的挖掘分析，严格的运营监管，呼唤针对用户隐私的安全保护标准、法律法规、行业规范，期待从海量数据中合理发现和发掘商业机会和商业价值。

（2）电信行业

大量数据的产生、存储和分析，使得运营商在数据对外应用和开放过程中面临着数据保密、用户隐私、商业合作等一系列问题。运营商需要利用企业平台、系统和工具实现数据的科学建模，确定或归类这些数据的价值。由于数据通常散乱在众多系统中，信息来源十分庞杂，因此运营商需要进行有效的数据收集与分析，保障数据的完整性和安全性。在对外合作时，运营商需要能够准确地将外部业务需求转换成实际的数据需求，建立完善的数据对外开放访问机制。在此过程中，如何有效保护用户隐私，防止企业核心数据泄露，成为运营商对外开展大数据应用需要考虑的重要问题。因此，电信运营商的大数据安全需求是：确保核心数据与资源的保密性、完整性和可用性，在保障用户利益、体验和隐私的基础上充分发挥数据价值。

（3）金融行业

金融行业的系统具有相互牵连、使用对象多样化、安全风险多方位、信息可靠性、保密性要求高等特征。而且金融业对网络的安全性、稳定性要求更高，系统要能够高速处理数据，提供冗余备份和容错功能，具备较好的管理能力和灵活性，以应对复杂的应用。虽然金融行业一直在数据安全方面追加投资和技术研发，但是由于金融领域业务链条的拉长、云计算模式的普及、自身系统复杂度的提升以及对数据的不当利用，都增加了金融业大数据的安全风险。因此，金融行业的大数据安全需求是：对数据访问控制、处理算法、网络安全、数据管理和应用等方面提出安全要求，期望利用大数据安全技术加强金融机构的内部控制，提高金融监管和服务水平，防范和化解金融风险。

（4）医疗行业

随着医疗数据的几何倍数增长，数据存储压力也越来越大。数据存储是否安全可靠，已经关乎医院业务的连续性。因为系统一旦出现故障，首先考验的就是数据的存储、灾备和恢复能力。如果数据不能迅速恢复，而且恢复不到断点，则对医院的业务、患者满意度构成直接损害。同时，医疗数据具有极强的隐私性，大多数医疗数据拥有者不愿意将数据直接提供给其他单位或个人进行研究利用，而数据处理技术和手段的有限性也造成了宝贵数据资源的浪费。因此，医疗行业对大数据安全的需求是：数据隐私性高于安全性和机密性，同时需要安全和可靠的数据存储、完善的数据备份和管理，以帮助医生与病人进行疾病诊断、药物开发、管理决策、完善医院服务，提高病人满意度，降低病人流失率。

（5）政府组织

大数据分析在安全上的潜能已经被各国政府组织发现，它的作用在于能够帮助国家构建更加安全的网络环境。例如，美国进口安全申报委员会不久前宣布，通过 6 个关键性的调查结果证明，大数据分析不仅具备强大的数据分析能力，而且能确保数据的安全性。美国国防部已经在积极部署大数据行动，利用海量数据挖掘高价值情报，提

高快速响应能力,实现决策自动化。而美国中央情报局通过利用大数据技术，提高从大型复杂的数字数据集中提取知识和观点的能力,加强国家安全[3]。因此,政府组织对大数据安全的需求是：隐私保护的安全监管、网络环境的安全感知、大数据安全标准的制定、安全管理机制的规范等内容。

3 大数据环境安全

通过上述分析可知，各领域的安全需求正在发生改变,从数据采集、数据整合、数据提炼、数据挖掘、安全分析、安全态势判断、安全检测到发现威胁,已经形成一个新的完整链条。在这一链条中,数据可能会丢失、泄露、被越权访问、被篡改,甚至涉及用户隐私和企业机密等内容。通常,大数据安全具有以下 6 个方面的特征和问题。

(1)移动数据安全面临高压力

社交媒体、电子商务、物联网等新应用的兴起,打破了企业原有价值链的围墙，仅对原有价值链各个环节的数据进行分析,已经不能满足需求。需要借助大数据战略打破数据边界，使企业了解更全面的运营及运营环境的全景图[4]。但是,这显然会对企业的移动数据安全防范能力提出更高的要求。此外,数据价值的提升会造成更多敏感性分析数据在移动设备间传递,一些恶意软件甚至具备一定的数据上传和监控功能,能够追踪到用户位置、窃取数据或机密信息,严重威胁个人的信息安全,使安全事故等级升高。在移动设备与移动平台威胁飞速增长的情况下,如何跟踪移动恶意软件样本及其始作俑者，分析样本相互间关系,成为移动大数据安全需要解决的问题。

(2)网络化社会使大数据易成为攻击目标

在网络空间里，大数据是更容易被发现的大目标。一方面,网络访问便捷化和数据流的形成,为实现资源的快速弹性推送和个性化服务提供基础。正因为平台的暴露,使得蕴含着潜在价值的大数据更容易吸引黑客的攻击。另一方面,在开放的网络化社会,大数据的数据量大且相互关联,使得黑客成功攻击一次就能获得更多数据,无形中降低了黑客的进攻成本,增加了收益率[5]。例如,黑客能够利用大数据发起僵尸网络攻击,同时控制上百万台傀儡机并发起攻击,或者利用大数据技术最大限度地收集更多有用信息。

(3)用户隐私保护成为难题

大数据的汇集不可避免地加大了用户隐私数据信息泄露的风险。由于数据中包含大量的用户信息,使得对大数据的开发利用很容易侵犯公民的隐私,恶意利用公民隐私的技术门槛大大降低。在大数据应用环境下,数据呈现动态特征,面对数据库中属性和表现形式不断随机变化,基于静态数据集的传统数据隐私保护技术面临挑战。各领域对于用户隐私保护有多方面要求和特点,数据之间存在复杂的关联和敏感性,而大部分现有隐私保护模型和算法都是仅针对传统的关系型数据,不能直接将其移植到大数据应用中。

(4)海量数据的安全存储问题

随着结构化数据和非结构化数据量的持续增长以及分析数据来源的多样化,以往的存储系统已经无法满足大数据应用的需要。对于占数据总量 80%以上的非结构化数据,通常采用 NoSQL 存储技术完成对大数据的抓取、管理和处理。虽然 NoSQL 数据存储易扩展、高可用、性能好,但是仍存在一些问题。例如,访问控制和隐私管理模式问题、技术漏洞和成熟度问题、授权与验证的安全问题、数据管理与保密问题等[6]。而结构化数据的安全防护也存在漏洞,例如物理故障、人为误操作、软件问题、病毒、木马和黑客攻击等因素都可能严重威胁数据的安全性。大数据所带来的存储容量问题、延迟、并发访问、安全问题、成本问题等,对大数据的存储系统架构和安全防护提出挑战。

(5)大数据生命周期变化促使数据安全进化

传统数据安全往往是围绕数据生命周期部署的,即数据的产生、存储、使用和销毁。随着大数据应用越来越多,数据的拥有者和管理者相分离,原来的数据生命周期逐渐转变成数据的产生、传输、存储和使用[7]。由于大数据的规模没有上限,且许多数据的生命周期极为短暂,因此,传统安全产品要想继续发挥作用,则需要及时解决大数据存储和处理的动态化、并行化特征,动态跟踪数据边界,管理对数据的操作行为。

(6)大数据的信任安全问题

大数据的最大障碍不是在多大程度上取得成功,而是让人们真正相信大数据、信任大数据,这包括对别人数据的信任和自我数据被正确使用的信任。例如,近年来工资“被增长”、CPI“被下降”、房价“被降低”、失业率“被减少”,因百姓的切身感受与统计数据之间的差异以及国家和地方之间 GDP 数据严重不符，都导致了市场对统计数据的质疑。同时,大数据的信任安全问题也不仅是指要相信大数据本身,还包括要相信可以通过数据获得的成果。但是,要让人们相信和信任通过大数据模型获得的洞察信息却并不容易,而证明大数据本身的价值比成功完成一个项目要更加困难。因此,构建对大数据的安全信任至关重要,这

需要政府机构、企事业单位、个人等多方面共同建设和维护好大数据可信任的安全环境。

4 大数据安全内涵

基于以上大数据环境的安全分析，作者认为大数据安全应该包括两个层面的含义，如图 1 所示。

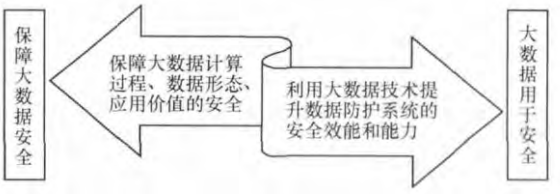

图 1 大数据安全内涵

(1)保障大数据安全，即大数据自身的安全问题

大数据安全不同于关系型数据安全，大数据无论是在数据体量、结构类型、处理速度、价值密度方面，还是在数据存储、查询模式、分析应用上都与关系型数据有着显著差异。大数据意味着数据及其承载系统的分布式，单个数据和系统的价值相对降低，空间和时间的大跨度、价值的稀疏，使得外部人员寻找价值攻击点更不容易。但是，在大数据环境下完全的去中心化很难，只要存在中心就可能成为被攻击的穴道，而对于低密度价值的提炼过程也是吸引攻击的内容。针对这些问题，传统安全产品所使用的监视、分析日志文件、发现数据和评估漏洞的技术在大数据环境中并不能有效运行。很多传统安全技术方案中，数据的大小会影响到安全控制或配套操作能否正确运行。多数安全产品不能进行调整，无法满足大数据领域，也不能完全理解其面对的信息。而且，在大数据时代会有越来越多的数据开放，交叉使用，在这个过程中如何保护用户隐私是最需要考虑的问题。图 2 说明了保障大数据安全的相关要点。

为解决大数据自身的安全问题，需要重新设计和构建大数据安全架构和开放数据服务，从网络安全、数据安全、灾难备份、安全风险管理、安全运营管理、安全事件管理、安全治理等各个角度考虑，部署整体的安全解决方案，保障大数据计算过程、数据形态、应用价值的安全。

(2)大数据用于安全，即用大数据解决安全问题

大数据在面临自身安全问题的同时，也给信息安全发展带来了新的机遇。2013 年 1 月，RSA/EMC 信息安全事业部发布的安全简报断言，大数据将会是整个安全行业发生重大转变的驱动因素，并将推动智能驱动的信息安全模型。预计到 2015 年，大数据分析将有可能给信息安全领域

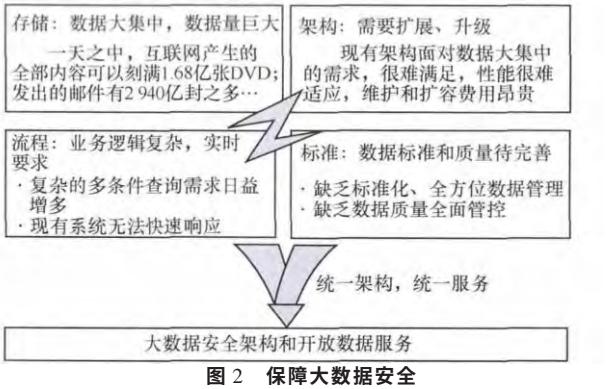

图 2 保障大数据安全

包括 SIEM(信息安全事件管理)、网络监控、用户身份认证和授权、身份管理、欺诈检测以及治理、风险及合规系统在内的大多数产品类别带来足以改变市场的变化。

大数据为安全分析提供新的可能性，对于海量数据的分析有助于更好地刻画网络异常行为，从而找出数据中的风险点，制定更好的预防攻击、防止信息泄露的策略。例如网络攻击行为总会留下蛛丝马迹，这些痕迹都以数据的形式隐藏在大数据中，利用大数据技术整合计算和处理资源有助于更有针对性地应对信息安全威胁，有助于找到攻击的源头。在此过程中，需要注意两个问题：一是大数据可能成为高级可持续攻击的载体；二是大数据分析技术也容易被黑客利用到攻击中去。需要明确大数据安全保障对象，加强对敏感和要害数据的监管，加快面向大数据的信息安全技术的研究，建立并完善大数据信息安全体系。

大数据也为企业提供一个更宽广的新视角，帮助它们更加前瞻性地发现安全威胁，利用大数据技术可以提升企业数据防护系统的安全效能、安全能力和安全效果。可以这样讲，大数据给信息安全带来的最大改变是通过自动化分析处理与深度挖掘，将之前很多时候亡羊补牢式的事中、事后处理，转向事前自动评估预测、应急处理，让安全防护主动起来。

目前，大数据在信息安全领域的应用包括两个方面：宏观上的网络安全态势感知和微观上的安全威胁发现[8]。前者是指运用大数据技术特有的海量存储、并行计算、高效查询等特点，解决大规模网络安全事件数据的有效获取，海量安全事件数据的实时关联分析，客观、可理解的网络安全指标体系建立等问题，从中发现主机和网络异常行为，起到全局安全预警的作用。后者是指从大数据中发现微观事件，特别是 APT 攻击发现。通过全面收集重要终端和服务器上的日志信息以及采集网络设备上的原始流

量，利用大数据技术进行分析和挖掘，检测并还原整个APT攻击场景，能够起到动态预防的安全作用，如图3所示。

5 应对策略

在大数据产业链的各个环节，安全问题无处不在，面对这一系列的安全风险和关键问题，如何保障大数据安全，并在信息安全领域有效利用，是企业需要认真解决的问题。只有大数据技术和大数据安全“两条腿”并行走路，大数据才可以真正成为企业的驱动力。根据传统信息安全成功经验及最新安全技术发展结果，作者认为可以从以下几方面开展大数据安全工作。

(1)构建大数据环境下的数据信息安全体系

数据信息安全是指数据信息的硬件、软件及数据受到保护，不因偶然的或者恶意的原因而遭到破坏、更改、泄露，系统连续可靠正常地运行，信息服务不中断。通常数据信息安全强调CIA三元组的目标，即保密性、完整性和可用性，另外还有一些其他目标，包括可追溯性、抗抵赖性、真实性、可控性等[9]。只有在正确完整的安全体系指导下，大数据信息安全建设所需的技术、产品、人员和操作等材料才能真正发挥各自的效力。设计大数据信息安全体系的目的在于：从管理和技术上保证数据安全策略得以完整准确的实现，全面准确地满足大数据安全需求。从具体内容上来看，该安全体系应该包含实现大数据环境下的信息安全所必需的功能或服务、安全机制和技术、管理和操作以及这些因素在整个体系中的合理部署和相互关系。所以，该安

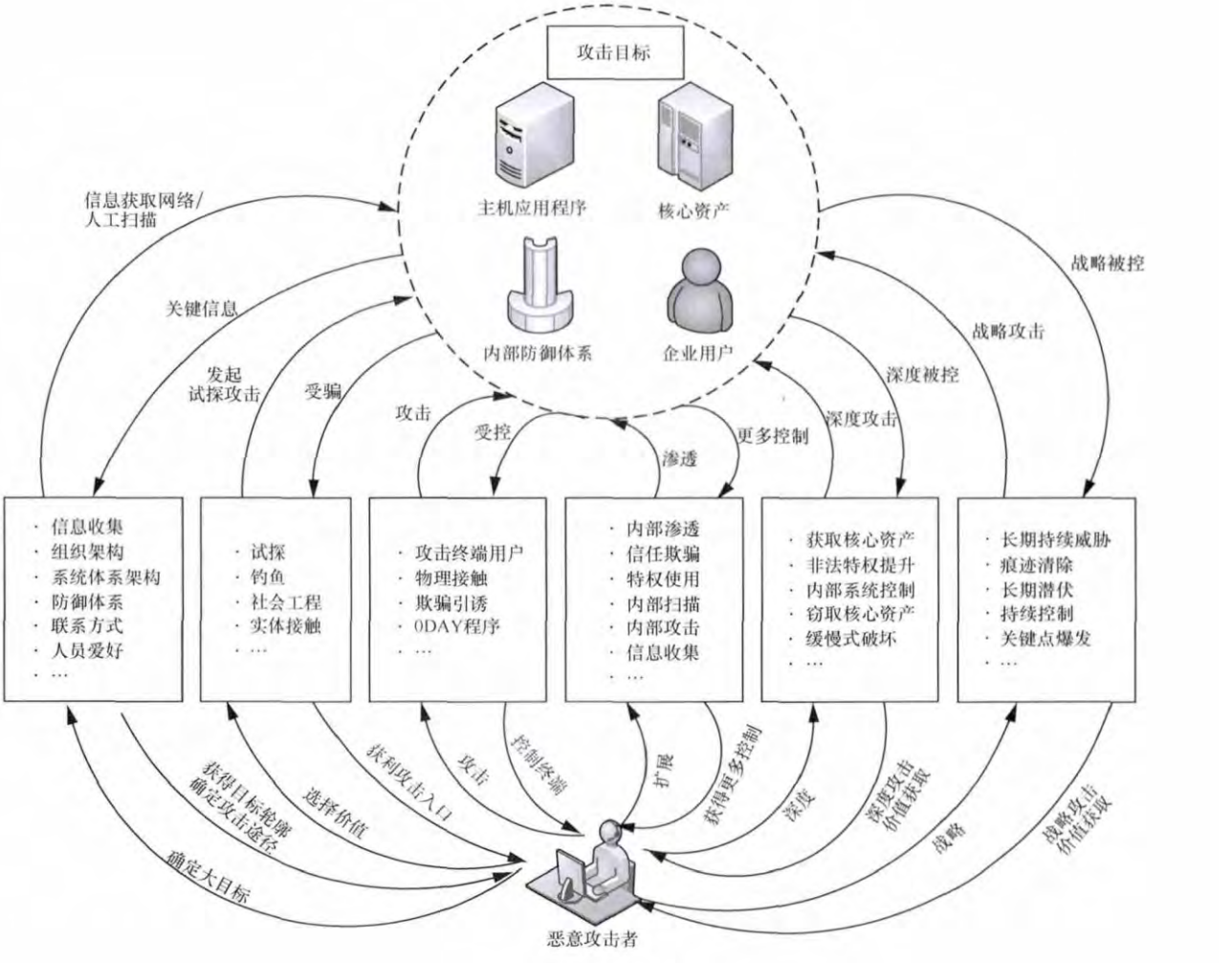

图3 大数据与APT攻击

全体系应该是多层次多方面的，必须能够完整描述大数据环境下的数据信息安全建设所要实现的最终形态。

大数据信息安全体系可以通过多种途径表示，例如非常具体的框架或者比较抽象的模型。无论表现形式如何，大数据信息安全体系都应该结合防护、检测、响应和恢复这几个关键环节在一起的动态发展的完整体系，能够为大数据安全的解决方案和工程实施提供参考和依据，帮助企业规范化、标准化大数据的安全防控内容和防护框架。

(2)研究保障大数据安全的关键技术

大数据安全保障技术可以从物理安全、系统安全、网络安全、存储安全、访问安全、审计安全、运营安全等角度进行考虑，围绕大数据全生命周期，即数据产生、采集、传输、存储、处理、分析、发布、展示和应用、产生新数据等阶段进行安全防护。其目标在于：最大程度地保护具有流动性和开放性特征的大数据自身安全，防止数据泄露、越权访问、数据篡改、数据丢失、密钥泄露、侵犯用户隐私等问题的出现。因此，大数据安全保障技术需要设计和构建更多的技术标准、安全规范、工具产品、安全服务等形式来保护大数据的安全。

(3)研究应用大数据安全的关键技术

通过了解大数据安全内涵和技术特点，可以在信息安全领域利用大数据分析技术，得到相关的安全预警和防护建议。例如，在大数据采集的基础上，企业可以从原始数据中进行二次提取，建立基础指标、应用层指标等多种类型指标，然后基于指标之间的关联分析、每个指标的变化状况，通过大数据分析帮助企业建立信誉评估机制，感知信息安全态势。

(4)加强大数据管理，做好安全评估，提高安全意识

通过技术保护大数据的安全必然重要，但安全管理制度也很关键。要从海量数据中提取价值，提高企业生产效率，就必须使用科学的大数据管理方法，降低各种安全隐患[10]。具体来说，可以从以下几个方面进行安全管理。

- 规范大数据建设。规范化建设可以促进大数据管理过程的正规有序，实现各级各类信息系统的网络互连、数据集成、资源共享，在统一的安全规范框架下运行。
- 完善大数据资产管理。大数据资产管理要能够清楚地定义数据元素，包括数据格式、别名、统计表以及其他特性标识符等；描述数据元素定义的信息来源及其相关数据元素的信息；记录使用信息，包括数据元素的产生及修改信息、安全及访问控制信息、访问历史记录。
- 建立以数据为中心的安全系统。为了确保数据中心系统的安全，防护系统主要通过防火墙、入侵检测系统、安全审计、抵抗拒绝服务攻击、流量整形和控制、网络防病毒系统来实现全面的安全防护。同时，通过使用加密、识别管理并结合其他主动安全管理技术，贯穿于数据从使用到迁移、停用的全部过程。
- 做好大数据安全风险评估。不同类型的数据形式以及数据的不同状态，都有其不同的泄密风险层级。针对大数据的固有特点，可以将其分为不同的安全风险等级，从而加强安全防范，并在实际生产中明确安全风险治理目标，降低企业数据泄露风险，分析并消除信息安全盲点。
- 提高企业员工安全意识。需要提升员工对大数据安全威胁的识别能力，了解正在使用的数据的价值，充分认识到自己在企业数据安全中的重要角色。企业也需要对员工进行安全培训，让员工对彼此在安全防护中的职责和战略有所了解，并结合周期性的安全攻击演习，以检验培训的成果。

6 结束语

本文梳理了互联网、电信、金融、医疗、政府组织五大行业的大数据安全需求，分析出大数据环境下的 6 个安全特征和问题，即移动数据安全、易攻击目标、用户隐私保护难题、安全存储问题、数据安全进化、信任安全问题等。随后，文中提炼出大数据的安全内涵，即保障大数据安全和应用大数据技术，并给出了相关的应对策略。

参考文献

1 The big data security gap: protecting the Hadoop custer challenges and opportunities with big data. http://www.zettaset.com/info-center/datasheets/zettaset_wp_security_0413.pdf

2 冯伟. 大数据时代面临的信息安全机遇和挑战. 中国科技投资, 2012(34): 49~53

3 王文超, 石海明, 曾华锋. 刍议大数据时代的国家信息安全. 国防科技, 2013, 34(2): 1~5

4 聂元铭. 大数据及其安全研究. 信息安全与通信. 2013(5): 15~16

5 杨建春. 网络环境下数据安全控制技术研究, 甘肃科技, 2011(16): 22~24

6 刘正伟, 张华忠, 文中领等. 海量数据持续数据保护技术研究及实现. 计算机研究与发展, 2012(s1): 37~41

7 郭三强, 郭燕锦. 大数据环境下的数据安全研究. 科技广场. 2013(2): 28~31

(下转第 122 页)

发环境和更灵活的资源调度。

· SaaS 应用模式是随需而变的，灵活地满足多种用户的不同需求。通过 SaaS 多租户特性，SDP 可为不同客户提供有针对性的服务。平台运营商提供统一的硬件、互联网带宽、操作系统、运营管理软件及各种能力资源系统，开发者使用平台提供的资源开发 SaaS 应用软件，并通过平台向最终用户交付 SaaS 服务。

4 结束语

移动互联网时代，传统以运营商为主导构建的 SDP 受到新型业务模式的冲击，运营商成为互联网开放平台的竞争者之一。保持运营商 SDP 平台的竞争力，必须要有核心能力吸引开发者，突破原有商业模式适应新型业务需求，随着市场需要实现对不同业务模式的灵活调整、灵活支撑。

作为移动互联网接入的必经通道，运营商也有其天然优势，拥有全程全网管道资源、全视图的数据资源。LTE 设备在标准上已要求支持 PCC（policy charging & control，内容识别和资源控制）功能，因此引入 LTE 后，智能管道网络基础就已具备，与云计算结合使得运营商 SDP 平台架构具有伸缩性，更加灵活和易于调整。SDP 聚合好这些优势资源，适应新的业务模式，优化生态环境，运营商 SDP 仍会保持其强大的竞争力，实现价值链共赢。

参考文献

1 董斌，王铮，魏民. 面向移动互联网的下一代业务网络. 北京：人民邮电出版社，2012

2 ETSI. Parlay X TS 29.199 Version 9.0.0, 2010

3 GSMA. OneAPI Version 2.0, 2010

4 吕斯基. 电信运营商 VS OTT：一种面向 OTT 价值服务的转型思路. http://www.huxiu.com/article/15160/1.html, 2013

5 杨勇，董振江，陆平. 具备云计算特性的业务交付平台及其关键技术研究. 中兴通讯技术，2011(17)

[作者简介]

董斌，男，中国电信股份有限公司上海研究院高级工程师，主要研究方向为移动业务网络 SDP 平台。

潘卫，男，中国电信股份有限公司北京研究院高级工程师，主要研究方向为业务网络规划、技术和分析。

王铮，男，中国电信股份有限公司上海研究院工程师，主要研究方向为移动业务网络及管理平台。

赵彦杰，男，中国电信股份有限公司上海分公司工程师，主要研究方向为业务平台的维护管理及产品支撑。

（收稿日期：2013-12-01）

（上接第 117 页）

8 潘柱廷. 高端信息安全与大数据. 信息安全与通信保密，2012(12)：19~20

9 严霄凤，张德馨. 大数据研究. 计算机技术与发展，2013(4)：168~172

10 杨高明，杨静，张健沛. 隐私保护的数据发布研究. 计算机科学，2011,38(9)：11~17

[作者简介]

胡坤，男，博士，中国联合网络通信集团有限公司博士后科研工作站高级工程师，主要研究方向为云计算、大数据应用、机器学习等。

刘镝，男，博士，中国联通研究院平台与云计算中心工程师，主要研究方向为信息安全、云计算、终端安全等。

刘明辉，女，博士，中国联通研究院平台与云计算中心工程师，主要研究方向为智能卡、版权保护、物联网安全技术、大数据安全等。

（收稿日期：2013-09-06）